UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/769,103	01/30/2004	Daniel M. Bodorin	MS307669.01/MSFTP2193US	9005

27195 7590 12/26/2008

AMIN, TUROCY & CALVIN, LLP
127 Public Square
57th Floor, Key Tower
CLEVELAND, OH 44114

EXAMINER
HAILU, TESHOME

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
12/26/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket1@thepatentattorneys.com
hholmes@thepatentattorneys.com
lpasterchek@thepatentattorneys.com

Office Action Summary	Application No.	Applicant(s)	
	10/769,103	BODORIN ET AL.	
	Examiner	Art Unit	
	TESHOME HAILU	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 December 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) *2,3,5 and 6* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 4 and 7-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on December 15, 2008 has been entered.

2. Claims 1, 4 and 7-24 have been amended.

3. Claims 2, 3, 5 and 6 are withdrawn form consideration

4. Claims 1-24 are pending.

Response to Amendment

5. Applicant's arguments with respect to claims 1, 4 and 7-24 have been considered but are moot in view of the new ground(s) of rejection.

6. Applicant's argument filed on December 15, 2008 with respect to the 35 USC 112 rejections to claims 10 and 14 have been fully considered in view of the amended claims and is persuasive. The 35 USC 112 rejections to claims 10 and 14 have been withdrawn.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 1 and 4 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The specification fails to mention or teach the claim limitation ".....returns an unpacked executable corresponding to the ***entire*** packed executable". The word "entire" is not in the specification. Appropriate correction is required.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1, 4 and 7-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lucas et al (US 6,968,461) in view of Thacker (US Pub. No. 2002/0035696) and further in view of Edwards (US 6,594,686).

As per claim 1 Lucas discloses:

A computer implemented system for determining whether a packed executable is malware, the system comprising: (column 3, line 63-67, FIG. 2 illustrates virus scanning operation when access is made to a compressed computer file 18. In order that this compressed computer file 18 can be properly checked it is decompressed into an uncompressed file form 20 and then a sequence of tests corresponding to separate DAT driver files within the virus definition data 16 are applied to the uncompressed data).

Wherein the malware evaluator, upon receiving incoming data, can at least in part determine

whether the incoming data is a packed executable, and if so, the malware evaluator provides the packed executable to the unpacking module such that an unpacked executable can be received from the unpacking module such that the malware evaluator can determine whether the unpacked executable is malware. (Column 4, line 22-25, a determination is made as to whether or not the portion of data recovered from the computer file being scanned requires decompressing or unpacking prior to testing. If the data does require decompressing or unpacking, then this is performed at step 26).

A malware evaluator for determining whether incoming data is malware, wherein the incoming data directed to a computing device is intercepted by the malware evaluator; (column 2, line 50-55, a receiver operable to receive a request to scan a computer file for computer viruses; initiating logic operable to initiate a virus scanning operation upon said computer file).

Lucas does not explicitly disclose about intercepting the incoming data directed to a computer device. However, in the same field of endeavor, Thacker teaches this limitation as, (page 1, paragraph 9, the system comprises a computer 11 which is connected to the Internet or other network of computers 12, with a virus trap 13 connected between the computer and the network for preventing viruses from entering the computer from the network).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Lucas and include the a way of intercepting the incoming data is a malware using the teaching of Thacker in order to prevent a virus from entering the computer from the network (see paragraph 7 of Thacker).

An unpacking module that receives a packed executable from the malware evaluator and returns an unpacked executable corresponding to the entire packed executable; (column 4, line 22-25, a determination is made as to whether or not the portion of data recovered from the computer file being scanned requires decompressing or unpacking prior to testing. If the data does require decompressing or unpacking, then this is performed at step 26).

Lucas and Thacker does not explicitly disclose about unpacking the entire packed executable. However, in the same field of endeavor, Edwards teaches this limitation as, (column , line , the archive

stores the embedded data files in a compressed format, and therefore it is necessary to decompress the archive (partially or completely) in order to test each of the embedded archive files for viruses).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Lucas and Thacker to include the system of unpacking the entire packed executable using the teaching of Edwards in order to substitute one method for the other to achieve the same end result of unpacking (decompressing) the packed (compressed) file.

Claim 4 is rejected under the same reason set forth in rejection of claim 1:

As per claim 7 Lucas in view of Thacker and further in view of Edwards discloses:

The system of Claim 1, wherein the returned unpacked executable corresponding to the packed executable is based at least in part on code or data derived from employing an unpacker other than the loader/unpacker received with the packed executable. (Column 3, line 1-6, the anti-virus system 12 requests a portion of the compressed file 18 to be decompressed and then applies the tests to that decompressed portion. If further portions still requiring checking, then more of the compressed file is decompressed and checked).

Claims 8, 20 and 21 are rejected under the same reason set forth in rejection of claim 7:

As per claim 9 Lucas in view of Thacker and further in view of Edwards discloses:

The system of Claim 1, wherein the intercepted incoming data resides only in one or more logically or physically isolated memory stores such that the intercepted incoming data can be located at a computer but does not actually "reach" the computer. Thacker discloses about intercepting incoming data as, (page 1, paragraph 9, the system comprises a computer 11 which is connected to the Internet or other network of computers 12, with a virus trap 13 connected between the computer and the network for preventing viruses from entering the computer from the network).

Claims 10, 14 and 22 are rejected under the same reason set forth in rejection of claim 9:

As per claim 11 Lucas in view of Thacker and further in view of Edwards discloses:

The system of Claim 1, wherein the unpacked executable generated by the unpacking module corresponds to a complete packed executable and not just a portion thereof. (Column 4, line 22-25, a determination is made as to whether or not the portion of data recovered from the computer file being scanned requires decompressing or unpacking prior to testing).

Claim 24 is rejected under the same reason set forth in rejection of claim 11:

As per claim 12 Lucas in view of Thacker and further in view of Edwards discloses:

The system of Claim 11, wherein the generated unpacked executable corresponding to a complete unpacked executable is unpacked without executing any portion thereof. (Column 4, line 22-25, a determination is made as to whether or not the portion of data recovered from the computer file being scanned requires decompressing or unpacking prior to testing).

Claim 23 is rejected under the same reason set forth in rejection of claim 12:

As per claim 13 Lucas in view of Thacker and further in view of Edwards discloses:

The system of Claim 1, wherein the malware evaluator determines whether the incoming data is malware without unpacking the incoming data if the incoming data is determined not to be a packed executable. (See fig. 6 of Lucan about scanning with out the decompression and unpacking).

Claims 15 and 19 are rejected under the same reason set forth in rejection of claim 13:

As per claim 16 Lucas in view of Thacker and further in view of Edwards discloses:

The system of Claim 15, wherein anti-virus software can be employed in determining whether the incoming data is malware. (Column 5, line 28-31, a portion of the computer file 64 to be tested is then subject to the processing associated with a series of DAT drivers within the computer virus definition data 16 of the anti-virus system 12).

As per claim 17 Lucas in view of Thacker and further in view of Edwards discloses:

The system of Claim 16, wherein the determining by anti-virus software can be by signature or pattern recognition processes. (Paragraph 50-55, within the anti-virus system 12, an anti-virus engine 14 working with virus definition data 16 serves to apply a plurality of tests for different known viruses and virus like behaviors to the computer file in order to detect the presence of a computer virus within that computer file).

As per claim 18 Lucas in view of Thacker and further in view of Edwards discloses:

An electronic device comprising the system of Claim 1, such that the electronic device can be placed between a network and a computer device to facilitate intercepting data directed to a computing device. (page 1, paragraph 9, the system comprises a computer 11 which is connected to the Internet or other network of computers 12, with a virus trap 13 connected between the computer and the network for preventing viruses from entering the computer from the network).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TESHOME HAILU whose telephone number is (571)270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Teshome Hailu

December 16, 2008

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434